


| | | | | |
|---------------------------|--------------------------------|---------------------------------|------------------|---|
| Category | IT Infrastructure and Services | Policy Number | SUP-ITS-205 |  جامعة زايد ZAYED UNIVERSITY |
| Classification | Public | Version | 3.0 | |
| Responsible Office | CAFO | Policy Owner | ITD Director | |
| Date Approved | 28 January 2025 | Effective Date | 17 February 2025 | |
| Date Last Reviewed | 22 June 2023 | Due Date for Next Review | 28 January 2028 | |

POLICY

Password Security

1. Purpose

The purpose of this Password Security policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the user authentication mechanism (i.e., user ID and password) at Zayed University.

2. Scope of Application

This policy applies to Zayed University faculty members, staff members, students, third-party contractors, vendors, and any such entity that is associated with Zayed University information, data, software, resources, and hardware and related processing facilities, and in anyway interacts with the information assets of the University.

3. Definitions

| | |
|-------------------|--|
| CAFO | University Chief Administration and Finance Officer |
| ITD | University Information Technology Department |
| MFA | Multi-Factor Authentication |
| TDRA | UAE Telecommunications and Digital Government Regulatory Authority |
| University | Zayed University |

4. Policy

4.1 All passwords, including initial passwords, must be constructed, and implemented in accordance with Zayed University's ("**University**") IT Department's ("**ITD**") information security management rules.

4.2 Users are responsible for all activity performed with their individual user-ID. User-IDs may not be utilized by anyone other than the user to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users must not perform any activity with IDs belonging to other users.

4.3 Users should not circumvent password entry with auto logon, application remembering, embedded scripts, or hard coded passwords in client software.

Exceptions may be made for specific IT applications (e.g., automated backup, laptop re-imaging software) with the approval of the ITD Director.

- 4.4** User accounts that have system-level privileges granted through group memberships or programs (e.g., sudo, or Domain Admins) must have a unique password for each account that is clearly different from the passwords used for all other accounts held by that user.
- 4.5** All system-level passwords (e.g., root, enable, network administrator, and application administration accounts) must be changed at least once every 15 days to reduce the risk of compromise.
- 4.6** All system-level password changes must be pre-approved by the appropriate manager.
- 4.7** Passwords stored in electronic format (e.g., in a database, spreadsheet, or other file) should be encrypted to prevent easy disclosure.
- 4.8** Passwords must not be divulged to anyone. ITD and IT contractors will not ask for user account passwords.
- 4.9** If the security of a password is in doubt, the password must be changed immediately.
- 4.10** University network administrators must not circumvent this policy for any reason.
- 4.11** Computing devices must not be left unattended without enabling a password protected screensaver or logging off the device.
- 4.12** The passwords for the servers, critical services, and network devices must always be stored in envelopes in a secure safe box. Access to the safe box is restricted to appropriate administrative roles within ITD (ITD Director, IT Infrastructure Manager, System Administrator, Network Manager, Network Administrator and Application Manager).
- 4.13** ITD will require users to change their passwords once every 90 days.
- 4.14** ITD will enforce Password History to discourage Users from alternating between several common passwords.
- 4.15** ITD will enforce user account management controls to lock user accounts after a defined number of failed authentication attempts.
- 4.16** ITD will provide guidelines/manuals for the implementation of this policy.
- 4.17** ITD will restrict the use of commonly used passwords (example: zayed123, zayed@123, etc.).
- 4.18** ITD will enable Multi-Factor Authentication (“MFA”) for all systems that support MFA.

4.19 Users must populate an alternate e-mail address and/or mobile number, through the university’s portal, to utilize the university’s Forgotten Password functionality.

5. Related Policies and Laws

- SUP-ITS-203 Information Security
- Telecommunications and Digital Government Regulatory Authority (TDRA) Regulations for Information Technology Security in Federal Entities

6. Administration

This policy is administered by the ITD.

7. Revision History

| Date | Revision | Ver. |
|------------------|---|-------------|
| 17 February 2025 | Chair of the Board’s Decision issued (PD#3 of 2025). | 3.0 |
| 28 January 2025 | Approved by FAIAC. | |
| 22 June 2023 | Endorsed by the Executive Committee. | |
| 20 February 2023 | Administrative change: <ul style="list-style-type: none"> • Updated the information header and policy numbers to be in line with the new format. • Updated the policy number from SUP-ITS-06 to SUP-ITS-205. | |
| 9 September 2022 | Revision: <ul style="list-style-type: none"> • Removed minimum password age restriction in order to accommodate the implementation of the Self-Service Password Portal (previous 3.14). • Added 3.17, 3.18, and 3.19. | |
| 4 October 2020 | President’s Decree issued (PD#90 of 2020). | 2.0 |
| 12 March 2018 | New policy approved by the University Council. | 1.0 |